How Much Redundancy is too Much Redundancy?

November, 2017

Adam Harden, QD35, Bastion Technologies Incorporated

Background

- Redundancy can be incorporated into systems that perform safety and non-safety functions to improve system reliability. Safety systems are of particular importance on a space vehicle due to the environment during flight.

- From an outsider's perspective, it would seem that adding redundant trains into a system would increase the reliability of that system by a factor equal to the number of redundant trains, or does it?

- The aerospace industry often has limitations on weight, space, cost, and schedule, so a better understanding of the impact redundancy has on reliability can result in more appropriate design decisions.

Approach

- Common Cause Failure (CCF) events will be defined in order to estimate the Probability of Failure (PoF) and reliability of each combination for an example system.
  - A CCF is a failure where two or more items fail within the mission time from a common failure mechanism. They are known and documented phenomenon that limit the benefit of system redundancy as a design approach to achieve high reliability.
  - Note that due to a lack of launch and CCF data in the aerospace industry, generic rate based data (Ref. U.S. Nuclear Regulatory Commission [NRC] NUREG/CR-5496, "CCF Parameter Estimates 2012") from the nuclear industry for the Alpha Factor method (Ref. U.S. NRC NUREG/CR-5485, "Guidelines on Modeling CCFs in Probabilistic Risk Assessment") is used.

- Analyze up to an eight redundant train combinations of a communication line system on a space vehicle, where success is any one train succeeds, to determine the reliability and PoF of each combination. Perform a comparison of the different combinations to demonstrate the decreasing return on reliability.

- The communication system's function on the space vehicle is to share data between a remote terminal and the vehicle's computer. Only reliability and PoF of the communication lines are considered in this analysis. Electrical boxes, communication cards, couplers, etc. are excluded.

- Reliability/failure rate data used for in the approach uses a notional value for demonstration purposes.

Analysis

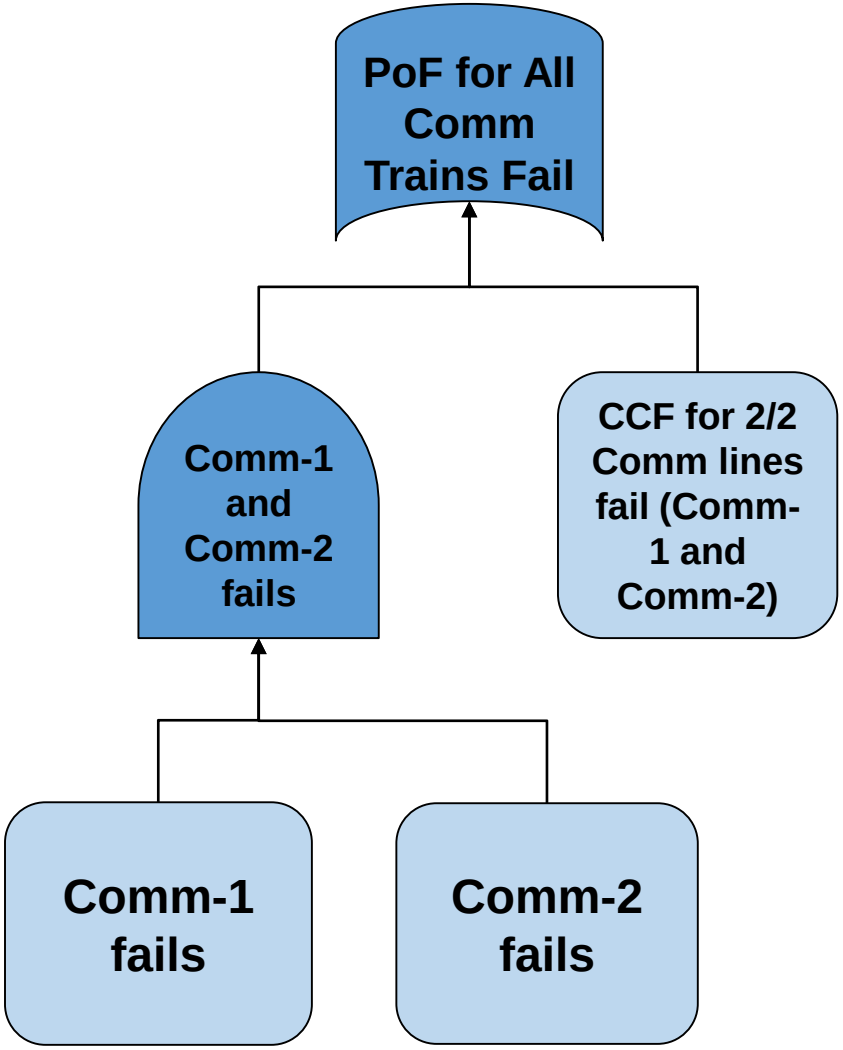
- The below diagram shows a 1-train line system that communicates data between a space vehicle's computer and a remote terminal connected directly to it.

- The table below presents the estimated reliability and Probability of Failure (PoF) of the communication line.

Success Criteria	Reliability	Failure Criteria	PoF
1 of 1	0.999	1 of 1	1.00E-3 (1 in 1,000)

Probability of Failure (PoF) and Reliability Calculations for Multiple Trains

- The fault tree to the right presents the logic for failure of comm-1 and comm-2
- The PoF for the top gate is:
  - Common Cause Failure (CCF) for 2 of 2 Comm lines, OR
  - Comm-1 AND Comm-2 fail
- For this example, the CCF probability is the product of the independent failure probability and the alpha factor for the failure combination 2 of 2 for generic rate based events
  - The alpha factor method develops CCF frequencies from a set of failure ratios and the total component failure rate
  - Alpha factors are derived from nuclear industry data and represent the percentage of the total failure rate for a specific failure combination
  - For this example, the alpha factor is a percentage of the total failure rate for the failure combination 2 of 2 (2 failures of a group size of 2)
- To calculate Reliability:
  - Reliability = 1 – PoF
- Similar logic is used to incorporate additional trains



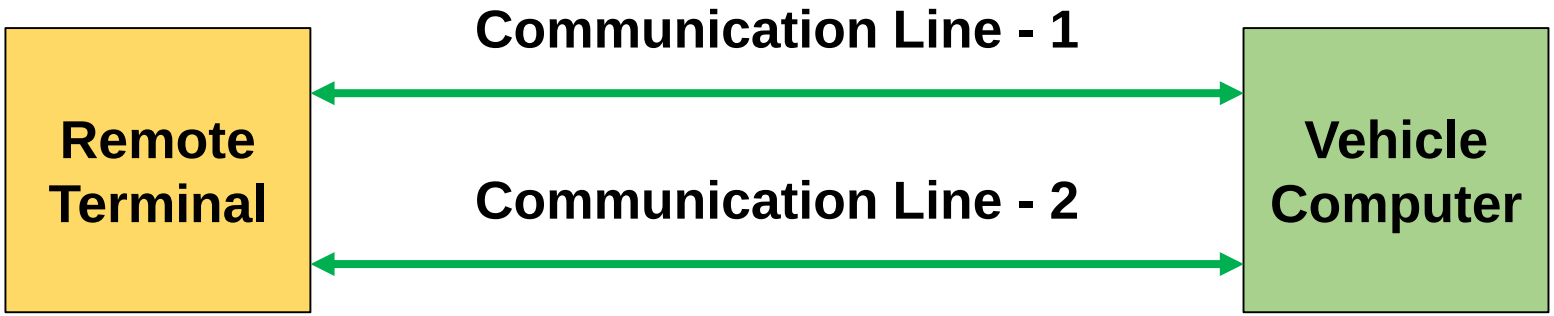
Alpha Factor Values for Common Cause Failure Calculations

- The table below presents the calculated Alpha Factor values, of specific failure combinations, for generic rate based events

Group Size	Success Criteria	Failure Criteria	Alpha Factor
2	1 of 2	2 of 2	6.88E-02
3	1 of 3	3 of 3	4.12E-02
4	1 of 4	4 of 4	2.52E-02
5	1 of 5	5 of 5	1.68E-02
6	1 of 6	6 of 6	1.30E-02
7	1 of 7	7 of 7	7.17E-03
8	1 of 8	8 of 8	4.29E-03

Analysis (continued)

- The below diagram shows a 2-train communication line system that communicates data between a space vehicle's computer and a remote terminal connected directly to it.



- The table below presents the estimated reliability and PoF of the 2-train communication line system.

Success Criteria	Reliability	Failure Criteria	PoF	% Change in Reliability
1 of 1	0.999	1 of 1	1.00E-3 (1 in 1,000)	NA
1 of 2	0.99993	2 of 2	6.98E-5 (1 in 14,300)	93.0%

Results

- The table below presents the estimated reliability and Probability of Failure (PoF) of all train configurations (where only 1 success is required) up to 8 trains.

Success Criteria	Reliability	Failure Criteria	PoF	% Change in Reliability from a Single Train	% Change in Reliability from Each Additional Train
1 of 1	0.999	1 of 1	1.00E-03 (1 in 1,000)	NA	NA
1 of 2	0.99993	2 of 2	6.98E-05 (1 in 14,300)	93.0%	93.0%
1 of 3	0.999959	3 of 3	4.12E-05 (1 in 24,300)	95.9%	2.9%
1 of 4	0.999975	4 of 4	2.52E-05 (1 in 39,700)	97.5%	1.6%
1 of 5	0.999983	5 of 5	1.68E-05 (1 in 59,500)	98.3%	0.8%
1 of 6	0.999987	6 of 6	1.30E-05 (1 in 76,900)	98.7%	0.4%
1 of 7	0.999993	7 of 7	7.17E-06 (1 in 139,400)	99.3%	0.6%
1 of 8	0.999996	8 of 8	4.29E-06 (1 in 233,200)	99.6%	0.3%

Largest increase in reliability comes from the addition of a second train. Note that the percent change in reliability from each additional train is reduced at each interval, except from a group size of 6 to 7.

Summary and Conclusions

- Adding a redundant train (i.e. a second train) in this example improves the reliability by 93%

- Increasing the number of redundant trains thereafter has marginal increases in reliability (6.6% increase in reliability from 2-trains to 8-trains)

Adding redundancy does not increase the reliability by a factor equal to the number of redundant trains that are incorporated.

In the aerospace industry where space, weight, cost, and schedule are important factors, it is best to consider the returns on reliability with respect to added redundancy. In this example, the reliability is increased with each added train, however there is less than a 1% return in reliability when an additional train is added after 4-trains. Therefore, adding further redundancy after 4-trains returns slight gains in reliability, decreases space on the vehicle, increases weight and cost, and pushes back schedule.